УТВЕРЖДАЮ:

Проректор по научной работе и инновациям, к.т.н., доцент

_____ А.Г. Лощилов

«_11_» _апреля_ 2022 г.

ЗАКЛЮЧЕНИЕ

Федерального государственного бюджетного образовательного учреждения высшего образования «Томский государственный университет систем управления и радиоэлектроники».

Диссертация «Методика построения сетей квантового распределения ключей смешанной топологии» выполнена в федеральном государственном бюджетном образовательном учреждении высшего образования «Томский государственный университет систем управления и радиоэлектроники» на кафедре комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС).

В период подготовки диссертации соискатель Жиляев Андрей Евгеньевич обучался в очной аспирантуре в Федеральном государственном бюджетном образовательном учреждении высшего образования «Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет)» на кафедре информационная безопасность. Во время обучения в аспирантуре Жиляев А.Е.. совмещал научную и педагогическую деятельность. В настоящее время он работает в младшего научного сотрудника Института системной интеграции и безопасности ТУСУР.

В 2016 году Жиляев А.Е. окончил Федеральное государственное бюджетное образовательное учреждение высшего образования «Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет)» по специальности «Компьютерная безопасность».

Справка о сдаче кандидатских экзаменов (иностранный язык, история и философия науки) выдана в 2021 г. Федеральным государственным бюджетным образовательным учреждением высшего образования «Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет)» и о сдаче кандидатских экзаменов (специальность) в 2022 г. Федеральным государственным бюджетным образовательным учреждением высшего образования «Томский государственный университет систем управления и радиоэлектроники».

Научный руководитель – Сабанов Алексей Геннадьевич, доктор технических наук, доцент, ведущий научный сотрудник Федерального государственного бюджетного образовательного учреждения высшего образования «Томский государственный университет систем управления и радиоэлектроники».

По итогам обсуждения принято следующее заключение:

Оценка выполненной соискателем работы.

Диссертация Жиляева А.Е. является законченным научным исследованием, содержит решение актуальной научно-технической задачи разработки методического обеспечения квантовых коммуникаций в части построения квантовых сетей смешанной топологии.

Актуальность темы и направленность исследования.

В диссертационной работе Жиляева А.Е. рассматривается применение технологии квантового распределения ключей для регулярного распределения общих секретов в пользовательские устройства. Актуальным является совершенствование методического обеспечения построения протяженных сетей квантового распределения ключей произвольной топологии для распределения общих секретов на неограниченные расстояния. Системы квантового распределения ключей имеют предельную максимальную длину квантового канала. Использование таких систем в сетях с доверенными промежуточными узлами позволяет распределять общие секреты на неограниченные расстояния по сети. Существующие методики предлагают передачу созданного квантового ключа некоторого сегмента, о котором у нарушителя уже имеется информация в силу квантового протокола, а также не рассматривают вопрос обеспечения целостности передаваемых секретов. Целью диссертационной работы является развитие методического обеспечения квантовых коммуникаций для повышения защищенности сетей квантового распределения ключей смешанной топологии.

Личное участие автора в получении результатов.

Постановка цели и задач научного исследования, подготовка двух публикаций по выполненной работе проводилась совместно с научным руководителем, д.т.н. Сабановым А.Г. Автором самостоятельно разработаны и реализованы: методика распределения квантовозащищенного ключа в сети квантового распределения ключей магистральной топологии и методика построения сети квантового распределения ключей смешанной топологии, проведена апробация разработанных методик.

Степень достоверности результатов диссертации.

Достоверность обеспечивается анализом современного состояния исследований в предметной области, обоснованием предложенных методик, не противоречащих известным положениям других авторов, апробацией полученных результатов в научных публикациях и докладах на международных и российских научных и научно-практических конференциях, положительным эффектом внедрения результатов в экспериментальные макеты сетей КРК (Университетская квантовая сеть, ViPNet QTS), промышленные комплексы систем КРК (ViPNet Quandor, ViPNet QSS, Квазар-СКР), а также использованием результатов работы в проектах документов национальной системы стандартизации.

Научная новизна диссертации.

В диссертации получены следующие новые научные результаты.

1. Разработана структура комплекса защищенной передачи данных, интегрированного с аппаратурой квантового распределения ключей, в том числе порядок функционирования такого комплекса для синхронизированной передачи ключевой информации в СЗИ, отличающийся от известных учетом целостности и конфиденциальности общих секретов в процессе передачи в СЗИ и контролем идентичности сформированных секретов, объединением классического канала аппаратуры КРК с транспортным каналом СЗИ для повышения защищенности классического канала аппаратуры КРК.

2. Разработана методика распределения общих секретов в сети КРК магистральной топологии, отличающаяся сохранением стойкости распределенных общих секретов при

компрометации квантовых ключей, а также возможностью сохранения конфиденциальности распределяемых секретов на промежуточных узлах сети КРК.

3. Предложена методика построения сети КРК смешанной топологии, включающая требования к структуре сети КРК, способу ее функционирования, методику распределения квантовозащищенных ключей (п. 2 новизны), отличающаяся от известных полностью децентрализованным управлением при создании квантовозащищенных ключей, учетом требований их целостности и конфиденциальности, а также имеющая по сравнению с зарубежными аналогами большую гибкость при масштабировании сети.

Практическая значимость диссертации.

Практическая значимость работы заключается в возможности создания промышленных образцов квантовых сетей, что соответствует, например, основным направлениям дорожной карты ОАО «РЖД» по развитию сквозной цифровой технологии квантовых коммуникаций. Предложенная структура базового сегмента сети КРК топологии «точка-точка» позволяет минимизировать число каналов между географически разнесенными узлами, что приводит к упрощению развертывания таких пар узлов.

Разработанные методики использованы при выполнении следующих проектов:

– комплексного проекта по созданию высокотехнологичного производства «Разработка и создание высокотехнологичного производства квантово-криптографической аппаратуры защиты информации», шифр 2017-218-09-8800, реализуемого по Соглашению № 03.G25.31.0254 от 27.04.2017 с Министерством образования и науки Российской Федерации;

– комплексного проекта «Разработка технологии и аппаратуры сетей квантового распределения криптографических ключей с использованием доверенных узлов», выполняемого по Соглашению с Министерством промышленности и торговли Российской Федерации № 020-11-2019-933 от 19.11.2019.

Разработанные в диссертации методики применены при разработке системы ViPNet QSS, Университетской квантовой сети, решения для протяженных квантовых сетей на базе изделия «Квазар-СКР».

Полнота изложенных материалов диссертации в печатных работах, опубликованных автором.

По материалам диссертации опубликовано 8 печатных работ, из которых в рекомендованных ВАК РФ периодических изданиях – 4. Две работы проиндексированы в Scopus и WoS. Получены 3 патента на изобретение РФ.

Работы, опубликованные в журналах, рекомендованных ВАК:

1. Реализация средства криптографической защиты информации, использующего квантовое распределение ключей / А.Г. Втюрина, В.Л. Елисеев, А.Е. Жиляев, А.С. Николаева, В.Н. Сергеев, А.В. Уривский// Доклады ТУСУР. – 2018. – Т. 21. – № 2. –С. 15–21.

2. Испытание комплекса квантовой криптографической аппаратуры защиты информации на городских волоконно-оптических линиях связи / А.В. Борисова, А.Е. Жиляев, С.В. Алферов, В.Л. Елисеев, Ю.В. Кармазиков, А.Н. Климов, К.А. Балыгин // Вестник российского нового университета. Серия: сложные системы: модели, анализ и управление. – 2019. – № 4. – С. 100–110.

3. Жиляев А.Е. Классификация схем выработки и распределения ключей в сетях квантового распределения ключей произвольной топологии // Доклады ТУСУР. – 2021. – Т. 24. – № 4. –С. 33–39.

4. Подход к формированию уровней доверия для оценки рисков ошибок аутентификации / А.Е. Жиляев, А.Г. Сабанов, П.А. Шелупанова, Д.С. Брагин, А.А. Мицель, М.Ю. Катаев // Вопросы защиты информации. –2022. – № 1. – С. 17–22.

В Scopus и WoS проиндексированы статьи:

5. Zhilyaev A.E. On the question of the authentication tag length based on reed-solomon codes / A.E. Zhilyaev, E.B. Gurova // Moscow Workshop on Electronic and Networking Technologies, MWENT 2018 - PROCEEDINGS. – 2018. –P. 1–5.

6. Borodin, M. Key generation schemes for channel authentication in quantum key distribution protocol / M. Borodin, A. Zhilyaev, A. Urivskiy // IET Quant. Comm. – 2021. – Vol. 2 – № 3. – P. 90– 97. – doi: 10.1049/qtc2.12020.

Другие работы, опубликованные по теме диссертации:

7. Жиляев А.Е. К вопросу об аутентификации классического канала в системах квантового распределения ключей // Безопасные информационные технологии: Сборник трудов Восьмой всероссийской научно-технической конференции. – Москва. – 2017. – С. 202–205.

8. Жиляев А.Е. Квантовое распределение ключей для защиты информации в городской сети банкоматов / А.Е. Жиляев, А.С. Николаева // Сборник научных работ участников ежегодной международной молодежной научно-практической конференции в рамках V Международного форума «Как попасть в пятерку?». Москва. – 2018. – С. 161–163.

Патенты на изобретения:

9. Пат. 2 708 511 РФ, МПК H 04 L 9/08, G 06 F 21/72. Способ формирования ключа между узлами вычислительной сети с использованием системы квантового распределения ключей / А.Е. Жиляев. – № 2019102923: заявл. 04.02.2019: опубл. 09.12.2019, Бюл. № 34. – 2 с.

10. Пат. 2 736 870 РФ МПК H 04 L 9/08. Комплекс для защищенной передачи данных в цифровой сети передачи данных с использованием однопроходной системы квантового распределения ключей и способ согласования ключей при работе комплекса / А.Г. Втюрина, А.Е. Жиляев. –№ 2019144324: заявл. 27.12.2019: опубл. 23.11.2020, Бюл. № 33. – 6 с.

11. Пат. 2 752 844 РФ, МПК H 04 L 9/08. Система выработки и распределения ключей и способ распределенной выработки ключей с использованием квантового распределения ключей (варианты) / А.Е. Жиляев. –№ 2020140774: заявл. 10.12.2020: опубл. 11.08.2021, Бюл. №23. – 9 с.

Соответствие содержания диссертации избранной специальности.

Диссертационная работа Жиляева А.Е. по своему содержанию соответствует профилю специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность», в частности, по следующим пунктам:

6. Модели и методы формирования комплексов средств противодействия угрозам хищения (разрушения, модификации) информации и нарушения информационной безопасности для различного вида объектов защиты вне зависимости от области их функционирования.

8. Модели противодействия угрозам нарушения информационной безопасности для любого вида информационных систем.

13. принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности.

Диссертация «Методика построения сетей квантового распределения ключей смешанной топологии» Жиляева Андрея Евгеньевича рекомендуется к защите на соискание ученой степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

Заключение принято на заседании научно-технического семинара «Интеллектуальные системы моделирования, проектирования и управления» кафедры комплексной информационной безопасности электронно-вычислительных систем факультета безопасности Федерального государственного бюджетного образовательного учреждения высшего образования «Томский государственный университет систем управления и радиоэлектроники».

Присутствовало на заседании 23 чел. Результаты голосования: «за» – 23 чел., «против» – 0 чел., «воздержалось» – 0 чел., протокол № 367 от 09 апреля 2022 г.

Заместитель председателя семинара,
доктор техн. наук, профессор,
профессор каф. КИБЭВС _____ И.А. Ходашинский

Ученый секретарь семинара,
канд. техн. наук, доцент каф. КИБЭВС _____ Е.Ю. Костюченко